2022 Midyear Market Outlook

Cyber Insurance

The past year has seen a rapidly hardening cyber insurance market as cyberattacks have surged in both cost and frequency. This increase in attacks has, in turn, resulted in a rise in cyber insurance claims and subsequent underwriting losses. Amid these market conditions, most policyholders experienced higher cyber insurance rates at their 2022 renewals, with many insureds seeing double-digit rate increases. In fact, industry data shows that rates rose by as much as 50%-100% during the first quarter of the year, depending on policyholders' specific exposures, loss history and risk management measures. Insureds have also begun encountering coverage restrictions, further scrutiny from underwriters regarding cybersecurity practices and exclusions for losses stemming from certain types of cyber incidents—namely, acts of cyberwarfare related to international conflicts and other increasingly prevalent cyberattack methods (e.g., ransomware). Looking ahead, policyholders who fail to adopt proper cybersecurity protocols or experience a rise in cyber-related losses may continue to face rate increases and coverage limitations for the foreseeable future.

Developments and Trends to Watch

Increased nation-state threats and coverage exclusions—Nation-state cyberattacks have become a growing concern over the past year, especially as the ongoing Russia-Ukraine conflict contributes to global cyberwarfare worries. In March 2022, the White House issued a statement warning U.S. organizations that nation-state cybersecurity exposures stemming from Russian attackers would likely increase in the coming months. The federal government also introduced new initiatives to harden the nation's cyber defenses against foreign threats and urged businesses to follow suit. Apart from elevating their cyber defenses, some insureds have sought coverage for emerging cyberwarfare risks. But, these policyholders have likely faced challenges obtaining such coverage, primarily due to war exclusions, which generally state that damages from "hostile or warlike actions" by a nation-state or its agents won't receive coverage. Cyber insurance policies are not immune to war exclusions. However, recent court cases and insurance industry shifts have both broadened and narrowed aspects of the scope of war exclusions as they pertain to cyberwarfare, creating confusion and posing potential insurance gaps among policyholders.

Elevated ransomware concerns—Ransomware attacks have skyrocketed in recent years, affecting many businesses but especially small- and medium-sized establishments. Yet, according to industry data, ransomware activity decreased by 20% in the first quarter of 2022 compared to the fourth quarter of 2021. This is likely due to international law enforcement operations disrupting several high-profile ransomware groups since the beginning of the year. Nevertheless, industry data confirmed that ransomware attacks still contributed to 32% of overall cyber-related losses in the first quarter of 2022. Further, costs stemming from ransomware attacks remain on the rise. According to data from cybersecurity company Palo Alto Networks, the average ransom payment reached $925,162 in the first five months of 2022—up 71% from last year.

Heightened business email compromise (BEC) risks—BEC scams entail a cybercriminal impersonating a legitimate source within an organization to trick their victim into wiring money, sharing sensitive data or engaging in other compromising activities. These scams are among the most expensive types of social engineering losses, and they have emerged as a major threat. According to the FBI, BEC scams caused more than $43 billion in losses since 2016, with such losses increasing by 65% between 2019 and 2021 alone.

Tips for Insurance Buyers

- Work with trusted insurance professionals to secure cyber coverage that meets your unique needs.
- Start the cyber insurance renewal process as early as possible and be prepared to complete supplemental applications regarding your cybersecurity practices.
- Take advantage of loss control services offered by insurance carriers to strengthen cybersecurity measures.
- Focus on employee training to prevent cybercrime from affecting your operations.
- Establish an effective, documented cyber incident response plan to minimize damages amid a cyberattack.